

**BURSOR & FISHER, P.A.**

Brittany S. Scott (State Bar No. 327132)  
Joshua R. Wilner (State Bar No. 353949)  
1990 North California Blvd., Suite 940  
Walnut Creek, CA 94596  
Telephone: (925) 300-4455  
Facsimile: (925) 407-2700  
E-mail: bscott@bursor.com  
jwilner@bursor.com

**BURSOR & FISHER, P.A.**

Philip L. Fraietta (State Bar No. 354768)  
1330 Avenue of the Americas, 32nd Floor  
New York, NY 10019  
Telephone: 646-837-7150  
Facsimile: (212) 989-9163  
E-Mail: pfraietta@bursor.com

**DRURY LEGAL, LLC**

Scott R. Drury (State Bar No. 355002)  
6 Carriage Lane  
Highwood, Illinois 60040  
Telephone: (312) 358-8225  
E-mail: scott@drurylegal.com

*Attorneys for Plaintiff*

**UNITED STATES DISTRICT COURT  
NORTHERN DISTRICT OF CALIFORNIA**

JONATHON PERRY-HUDSON, individually  
and on behalf of all others similarly situated,

Plaintiff,

v.

TWILIO, INC.,

Defendant.

Case No.

**CLASS ACTION COMPLAINT**

JURY TRIAL DEMANDED

1 Plaintiff Jonathon Perry-Hudson (“Plaintiff”) brings this action on behalf of himself and all  
2 others similarly situated against Twilio, Inc. (“Defendant”). Plaintiff makes the following  
3 allegations pursuant to the investigation of his counsel and based upon information and belief,  
4 except as to allegations specifically pertaining to themselves and their counsel, which are based on  
5 personal knowledge.

#### 6 **NATURE OF THE ACTION**

7 1. This is a class action suit brought against Twilio, Inc. (“Twilio” or “Defendant”) for  
8 wiretapping the electronic communications of visitors of keeps.com (the “Website” or “Keeps”).

9 2. Defendant intercepted communications sent and received by Plaintiff and Class  
10 Members, including communications containing personally identifying information (“PII”) and  
11 protected health information (“PHI”). Plaintiff brings this action for legal and equitable remedies  
12 resulting from these illegal actions.

#### 13 **PARTIES**

##### 14 ***Defendant***

15 3. Defendant Twilio, Inc. is a Delaware Corporation with its principal place of  
16 business at 101 Spear Street Suite 500, San Francisco, California 94105. Defendant owns and  
17 operates the Segment API, a piece of code installed on the Website that acts as a wiretap for  
18 Website visitors’ confidential communications. Defendant contracts with Keeps to enable the  
19 conduct at issue.

##### 20 ***Plaintiff***

21 4. Plaintiff Jonathon Perry-Hudson is a natural person and citizen of California,  
22 residing in San Diego, California.

23 5. On or around May 8, 2024, Plaintiff visited keeps.com to purchase prescription hair  
24 loss medication. As part of the purchase process, Plaintiff answered a series of questions related to  
25 his physical health. The questionnaire responses were given to a licensed medical provider who  
26 curated a customized treatment plan for Plaintiff.

27 6. Defendant intercepted Plaintiff’s communications, including those that contained  
28 personally identifiable information (“PII”), protected health information (“PHI”), and related

1 confidential information. Defendant intercepted Plaintiff's communications without Plaintiff's  
2 knowledge, consent, or express written authorization.

3 7. After placing his order from the Website, Plaintiff began receiving targeted  
4 advertisements related to hair loss products on Facebook and other internet sites.

### 5 **JURISDICTION AND VENUE**

6 8. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1332(d)(2)(A)  
7 because this case is a class action where the aggregate claims of all members of the proposed class  
8 are in excess of \$5,000,000, exclusive of interest and costs, and at least one member of the  
9 proposed class is a citizen of a state different from Defendant.

10 9. This Court has personal jurisdiction over Defendant because Defendant's principal  
11 place of business is in this District.

12 10. Pursuant to 28 U.S.C. § 1391, this Court is the proper venue for this action because  
13 Defendant resides in this District.

### 14 **FACTUAL ALLEGATIONS**

#### 15 **A. Background of the California Information Privacy Act ("CIPA")**

16 11. To establish liability under Cal. Penal Code § 631(a), a plaintiff need only establish  
17 that the defendant, "by means of any machine, instrument, contrivance, or in any other manner,"  
18 does any of the following:

19 Intentionally taps, or makes any unauthorized connection, whether physically,  
20 electrically, acoustically, inductively or otherwise, with any telegraph or telephone  
21 wire, line, cable, or instrument, including the wire, line, cable, or instrument of any  
internal telephonic communication system,

22 Or

23 Willfully and without the consent of all parties to the communication, or in any  
24 unauthorized manner, reads or attempts to read or learn the contents or meaning of  
25 any message, report, or communication while the same is in transit or passing over  
any wire, line or cable or is being sent from or received at any place within this state,

26 Or

27 Uses, or attempts to use, in any manner, or for any purpose, or to communicate in any  
28 way, any information so obtained

1 Or

2 Aids, agrees with, employs, or conspires with any person or persons to unlawfully  
3 do, or permit, or cause to be done any of the acts or things mentioned above in this  
4 section.

5 12. Section 631(a)'s applicability is not limited to phone lines, but also applies to "new  
6 technologies" such as computers, the internet, and email. *See Matera v. Google Inc.*, 2016 WL  
7 8200619, at \*21 (N.D. Cal. Aug. 12, 2016) (CIPA applies to "new technologies" and must be  
8 construed broadly to effectuate its remedial purpose of protecting privacy); *Bradley v. Google, Inc.*,  
9 2006 WL 3798134, at \*5-6 (N.D. Cal. Dec. 22, 2006) (CIPA governs "electronic  
10 communications"); *In re Facebook, Inc. Internet Tracking Litigation*, 956 F.3d 589 (9th Cir. 2020)  
11 (reversing dismissal of CIPA and common law privacy claims based on Facebook's collection of  
12 consumers' internet browsing history).

13 13. Under Cal. Penal Code § 637.2, Plaintiff and Class Members may seek injunctive  
14 relief and statutory damages of \$5,000 per violation.

15 **B. Federal Warning on Tracking Codes on Healthcare Websites**

16 14. The government previously issued a guidance warning that tracking codes like the  
17 Segment API may violate federal privacy law when installed on healthcare websites. In December  
18 2022, the Department of Health and Human Services' Office for Civil Rights ("OCR") issued a  
19 statement, titled "Use of Online Tracking Technologies by HIPAA Covered Entities and Business  
20 Associates" (the "Bulletin").

21 15. Healthcare organizations regulated under HIPAA may use third-party tracking tools,  
22 such as Twilio's Segment API, in a limited way, to perform analysis on data key to operations.  
23 They are not permitted, however, to use these tools in a way that may expose patients' PHI to these  
24 vendors. The Bulletin explains:

25 Regulated entities [those to which HIPAA applies] are not permitted to use tracking  
26 technologies in a manner that would result in impermissible disclosures of PHI to  
27 tracking technology vendors or any other violations of the HIPAA Rules. *For*  
28 *example, disclosures of PHI to tracking technology vendors for marketing*

1 *purposes, without individuals' HIPAA-compliant authorizations, would constitute*  
 2 *impermissible disclosures.*<sup>1</sup>

3 16. The Bulletin discusses the types of harm that disclosure may cause to the patient:

4 An impermissible disclosure of an individual's PHI not only violates the Privacy  
 5 Rule<sup>[fn]</sup> but also may result in a wide range of additional harms to the individual or  
 6 others. For example, an impermissible disclosure of PHI may result in identity theft,  
 7 financial loss, *discrimination, stigma, mental anguish, or other serious negative*  
 8 *consequences to the reputation, health, or physical safety of the individual or to*  
 9 *others identified in the individual's PHI.* Such disclosures can reveal incredibly  
 10 sensitive information about an individual, *including diagnoses, frequency of visits to*  
 11 *a therapist or other health care professionals, and where an individual seeks*  
 12 *medical treatment.* While it has always been true that regulated entities may not  
 13 impermissibly disclose PHI to tracking technology vendors, *because of the*  
 14 *proliferation of tracking technologies collecting sensitive information, now more*  
 15 *than ever, it is critical for regulated entities to ensure that they disclose PHI only as*  
 16 *expressly permitted or required by the HIPAA Privacy Rule.*<sup>2</sup>

17 17. Plaintiff and Class Members face just the risks about which the government  
 18 expresses concern for. When Plaintiff and Class Members filled out the questionnaire on the  
 19 Website, they believed their responses would only be used to obtain a recommendation for  
 20 prescription hair growth medication. In the questionnaire, Plaintiff provided information to a  
 21 healthcare provider about his medical condition for the purpose of obtaining prescription  
 22 medication. This information is, as described by the OCR in its bulletin, "highly sensitive."

23 18. The Bulletin goes on to make clear how broad the government's view of protected  
 24 information is. It explains:

25 This information might include an individual's medical record number, home or email  
 26 address, or dates of appointments, as well as an individual's IP address or geographic  
 27 location, medical device IDs, *or any unique identifying code.*<sup>3</sup>

28 19. Crucially, that paragraph in the government's Bulletin continues:

*All such [individually identifiable health information ("IIHI")] collected on a*  
*regulated entity's website or mobile app generally is PHI, even if the individual does*  
*not have an existing relationship with the regulated entity and even if the IIHI,*  
*such as IP address or geographic location, does not include specific treatment or*  
*billing information like dates and types of health care services.* This is because,  
*when a regulated entity collects the individual's IIHI through its website or mobile*  
*app, the information connects the individual to the regulated entity (i.e., it is*  
*indicative that the individual has received or will receive health care services or*

<sup>1</sup> *Id.* (Emphasis added.)

<sup>2</sup> *Id.* (Emphasis added.)

<sup>3</sup> *Id.* (Emphasis added.)

*benefits from the covered entity), and thus relates to the individual's past, present, or future health or health care or payment for care.*<sup>4</sup>

20. In July 2022, the Federal Trade Commission ("FTC") and OCR issued a joint press release warning healthcare providers about the privacy and security risks arising from the use of online tracking technologies:

The Federal Trade Commission and the U.S. Department of Health and Human Services' Office for Civil Rights (OCR) are cautioning [healthcare providers] and telehealth providers about the privacy and security risks related to the use of online tracking technologies integrated into their websites or mobile apps that may be impermissibly disclosing consumers' sensitive personal health data to third parties.

"When consumers visit a [healthcare provider's] website or seek telehealth services, they should not have to worry that their most private and sensitive health information may be disclosed to advertisers and other unnamed, hidden third parties," said Samuel Levine, Director of the FTC's Bureau of Consumer Protection. "The FTC is again serving notice that companies need to exercise extreme caution when using online tracking technologies and that we will continue doing everything in our powers to protect consumers' health information from potential misuse and exploitation."

"Although online tracking technologies can be used for beneficial purposes, patients and others should not have to sacrifice the privacy of their health information when using a [healthcare provider's] website," said Melanie Fontes Rainer, OCR Director. "OCR continues to be concerned about impermissible disclosures of health information to third parties and will use all of its resources to address this issue."

The two agencies sent the joint letter to approximately 130 [healthcare providers] and telehealth providers to alert them about the risks and concerns about the use of technologies, such as the Meta/Facebook pixel and Google Analytics, that can track a user's online activities. These tracking technologies gather identifiable information about users, usually without their knowledge and in ways that are hard for users to avoid, as users interact with a website or mobile app.

In their letter, both agencies reiterated the risks posed by the unauthorized disclosure of an individual's personal health information to third parties. For example, the disclosure of such information could reveal sensitive information including health conditions, diagnoses, medications, medical treatments, frequency of visits to health care professionals, and where an individual seeks medical treatment.

. . . Through its recent enforcement actions against BetterHelp, GoodRx and Premom, as well as recent guidance from the FTC's Office of Technology, the FTC has put companies on notice that they must monitor the flow of health information to third parties that use tracking technologies integrated into websites and apps. The unauthorized disclosure of such information may violate the FTC Act and could

---

<sup>4</sup> *Id.* (Emphasis added.)

constitute a breach of security under the FTC's Health Breach Notification Rule  
 ....<sup>5</sup>

21. Defendant's conduct, as alleged herein, is directly contrary to clear pronouncements by the FTC and OCR.

22. In light of, and in addition to, the government's own issued guidance above, news sources are also warning that tracking code, like Twilio's Segment API, poses risks of violating federal privacy law and HIPAA:

Federal regulators are warning [healthcare providers] and telehealth providers about the data privacy risks of using third-party tracking technologies.

These services, like [Facebook Tracking] Pixel or Google Analytics, could violate the Health Insurance Portability and Accountability Act (HIPAA) or Federal Trade Commission (FTC) data security rules, officials said.

The FTC and the U.S. Department of Health and Human Services' Office for Civil Rights (OCR) issued a rare joint release announcing that 130 [healthcare providers] and telehealth providers received a letter warning them about the data privacy and security risks related to the use of online tracking technologies integrated into their websites or mobile apps.... "The compliance buck still stops with you. Furthermore, your company is legally responsible even if you don't use the data obtained through tracking technologies for marketing purposes."<sup>6</sup>

Fierce Healthcare also spoke up in an April 3, 2023 article:

Nearly all nonfederal acute care [healthcare providers'] websites track and transfer data to a third party, potentially fueling the unwanted disclosures of patients' sensitive health information and opening up that [healthcare provider] to legal liability, according to a recently published University of Pennsylvania analysis. [<https://www.healthaffairs.org/doi/full/10.1377/hlthaff.2022.01205>]. The census of more than 3,700 [healthcare provider] homepages found at least one third-party data transfer among 98.6% of the websites as well as at least one third-party cookie on 94.3%, researchers wrote in Health Affairs.

The [healthcare providers'] homepages had a median of 16 third-party transfers... Many of these complaints cite Facebook parent company Meta's Pixel tracker, which a June 2022 investigation from The Markup [<https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites>] detected on about a third of [health care providers'] websites. That

<sup>5</sup> Federal Trade Commission, *FTC and HHS Warn Hospital Systems and Telehealth Providers about Privacy and Security Risks from Online Tracking Technologies*, July 20, 2023, <https://www.ftc.gov/news-events/news/press-releases/2023/07/ftc-hhs-warn-hospital-systems-telehealth-providers-about-privacy-security-risks-online-tracking>.

<sup>6</sup> Heather Landi, *Regulators warn hospitals and telehealth companies about privacy risks of Meta, Google tracking tech*, FIERCE HEALTHCARE, July 21, 2023, <https://www.fiercehealthcare.com/health-tech/regulators-warn-hospitals-and-telehealth-companies-about-privacy-risks-meta-google>.



report found evidence that, in some instances, the sensitive data transferred to third parties met the criteria for a HIPAA violation.<sup>7</sup>

Health Affairs also published an article in April 2023, stating:

By including third-party tracking code on their websites, [healthcare providers] are facilitating the profiling of their patients by third parties. These practices can lead to dignitary harms, which occur when third parties gain access to sensitive health information that a person would not wish to share. These practices may also lead to increased health-related advertising that targets patients, as well as to legal liability for [healthcare providers].<sup>8</sup>

23. On March 18, 2024, OCR published a revised version of the Bulletin, which further clarified that “identifying information showing [a patient’s] visit to [a public] webpage is a disclosure of PHI to the extent that the information is both identifiable and related to the individual’s health or future health care.”<sup>9</sup>

24. On July 20, 2023, the OCR and FTC sent Keeps, the owner and operator of the Website, a letter to draw attention to “serious privacy and security risks related to the use of online tracking technologies that may be present on [its] website or mobile application (app) and impermissibly disclosing consumers’ sensitive personal health information to third parties.” (Emphasis Added) A true and correct copy of the warning letter is attached hereto as Exhibit A. The letter went on to emphasize the serious nature of such disclosures:

Impermissible disclosures of an individual’s personal health information to third parties may result in a wide range of harm to an individual or others. Such disclosures can reveal sensitive information including health conditions, diagnoses, medications, medical treatments, frequency of visits to health care professionals, where an individual seeks medical treatment, and more. In addition, impermissible disclosures of personal health information may result in identity theft, financial loss, discrimination, stigma, mental anguish, or other serious negative consequences to the reputation, health, or physical safety of the individual or to others.

<sup>7</sup> Dave Muoio, *Almost every hospital’s homepage is sending visitors’ data to third parties, study finds*, FIERCE HEALTHCARE, Apr. 3, 2023, <https://www.fiercehealthcare.com/providers/almost-every-hospital-homepage-sending-visitors-data-third-parties-study-finds>.

<sup>8</sup> Ari B. Friedman, et al., *Widespread Third-Party Tracking On Hospital Websites Poses Privacy Risks For Patients And Legal Liability For Hospitals*, HEALTH AFFAIRS, Vol. 42, No. 24, April 2023, <https://www.healthaffairs.org/doi/10.1377/hlthaff.2022.01205>.

<sup>9</sup> HHS.gov, *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates*, <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html>.



25. On March 18, 2024, HHS published a revised version of the bulletin, which further clarified that “identifying information showing [a patient’s] visit to [a public] webpage is a disclosure of PHI to the extent that the information is both identifiable and related to the individual’s health or future health care.”

26. This is further evidence that the data that Defendant intercepted is protected Personal Information. The sharing of that information was a violation of Class Members’ rights.

### C. Overview of Twilio’s Segment API

27. Defendant Twilio is “a customer engagement platform used by hundreds of thousands of businesses and more than ten million developers worldwide to build unique, personalized experiences for their customers.”<sup>10</sup>

28. Twilio powers this platform through its Segment API, which offers “world-class customer data infrastructure, so [developers] can design hyper-personalized, omnichannel campaigns across all channels.”<sup>11</sup> In particular, once integrated into a developer’s website, the Segment API provides Twilio’s platform with “customer identification and segmentation,”<sup>12</sup> and it does this by “collecting and connecting data from other tools and aggregating the data to monitor performance, inform decision-making processes, and create uniquely customized user experiences.”<sup>13</sup>

29. Keeps.com utilizes the Segment API on its Website and sends its consumers’ PII to Twilio through the Segment API in order to assist with Keeps’ marketing, advertising, and analytics efforts.

30. Twilio entices developers to integrate the Segment API by underscoring its signature feature: “Engage.” Formerly known as Personas, Engage “is a powerful personalization

<sup>10</sup> *What is Twilio? An introduction to the leading customer engagement platform*, TWILIO, <https://www.twilio.com/en-us/resource-center/what-is-twilio-an-introduction-to-the-leading-customer-engagement-platform> (last accessed Apr. 12, 2024).

<sup>11</sup> TWILIO SEGMENT, <https://segment.com/twilio/>.

<sup>12</sup> Ingrid Lunden, *Twilio Confirms It Is Buying Segment For \$3.2b In An All-Stock Deal*, TechCrunch (Oct. 12, 2020), <https://techcrunch.com/2020/10/12/twilio-confirms-it-is-buying-segment-for-3-2b-in-an-all-stock-deal/>.

<sup>13</sup> Segment.io Defined, INDICATIVE, <https://www.indicative.com/resource/segment-io/>.

1 platform that helps you create unified customer profiles.”<sup>14</sup> Twilio creates these “unified customer  
2 profiles” by “tak[ing] event data from across devices and channels and intelligently merg[ing] it  
3 into complete user- or account-level profiles.”<sup>15</sup>

4 31. Twilio builds these personas through “Segment Identity Resolution.” This process  
5 “merges the complete history of each customer into a single profile, no matter where they interact  
6 with your business.” The Segment Identity Resolution supports, among other identifiers, “cookie  
7 IDs, device IDs, emails, and custom external IDs,” helping Twilio capture “a user’s interaction  
8 across web, mobile, server and third party partner touch-points in real-time[.]” The Segment  
9 Identity Resolution then combines these “multiple external IDs,” into “one persistent ID,”  
10 culminating into its offered Persona.

11 32. With Identity Resolution, Twilio associates a users’ AAID with a corresponding  
12 Persona Profile on Twilio’s platform. Because Twilio assembles information from other sources  
13 into the Persona Profile, AAID alone allows Twilio to identify a particular person.

14 33. Twilio leverages these profiles to assist its customers, like keeps.com, to enhance  
15 their marketing, advertising, and analytics efforts.

16 34. Keeps.com discloses users’ PII and PHI to Twilio through the Segment API so  
17 Twilio can better target its marketing campaigns. Keeps.com does this through Twilio’s  
18 “Audience” feature, which “group[s] users or accounts based on event behavior and traits that  
19 Segment tracks.”<sup>16</sup> In other words, the Audience feature allows for targeted marketing of  
20 advertisements at Engage profiles that fit specific parameters. As explained below, keeps.com  
21 builds these marketing campaigns through Defendant’s analytics services.

22 35. Keeps.com also discloses users’ PII and PHI to Twilio, through the Segment API, so  
23 it can better target advertisements. After keeps.com discloses users’ PII and PHI, Twilio compiles  
24 and transmits that information to other third parties that keeps.com utilizes for targeted

26 <sup>14</sup> Documentation, SEGMENT, <https://segment.com/docs/engage/>.

27 <sup>15</sup> *Id.*

28 <sup>16</sup> ENGAGE AUDIENCE OVERVIEW, SEGMENT, <https://segment.com/docs/engage/audiences/>.

advertising.<sup>17</sup> Twilio labels these companies “Segment Destinations,” which are tools that businesses use for personalization and marketing.<sup>18</sup> In this role, Twilio acts as a facilitator, compiling PII so developers can “personalize messages across channels, optimize ad spend, and improve targeting.”<sup>19</sup> When Twilio transmits PII and PHI to Meta, for example, it sends “an expanded list of identifiers or traits to [Meta], so that [Meta] can try to use these additional datapoints to match to their user profiles.”<sup>20</sup> The same goes for Google, with Twilio helping developers “run advertising campaigns without having to manually update the list of users to target in Adwords campaigns.”<sup>21</sup> Keeps.com utilizes Defendant’s API to amplify its advertising campaigns.

36. Twilio describes the above process as “building an Audience,” meaning it “group[s] users or accounts based on event behavior and traits that Segment tracks.”<sup>22</sup> As an example, Twilio lets developers “create[e] an ‘inactive accounts’ audience that lists paid accounts with no logins in 60 days.”<sup>23</sup> After, “developers can push the audience to your marketing and analytics tools.”<sup>24</sup>

37. In short, keeps.com utilizes the Segment API to analyze user data, launch marketing campaigns, and target specific users or specific groups of users for advertisements. In this case, the data used was information about Plaintiff’s and Class Members’ medical conditions and treatment.

#### **D. The Segment API Is Installed On The Website And Collects Visitors’ PII And PHI**

38. Defendant’s Segment API is deployed throughout the Website, including on all

<sup>17</sup> USING ENGAGE DATA, SEGMENT, <https://segment.com/docs/engage/using-engage-data/> (these third parties include Facebook, Google, and Salesforce).

<sup>18</sup> *Id.*

<sup>19</sup> *Id.*

<sup>20</sup> PERSONAS FACEBOOK CUSTOM AUDIENCES DESTINATION, SEGMENT, <https://segment.com/docs/connections/destinations/catalog/personas-facebook-custom-audiences/>.

<sup>21</sup> *Id.*

<sup>22</sup> ENGAGE AUDIENCES OVERVIEW, SEGMENT, <https://segment.com/docs/engage/audiences/>.

<sup>23</sup> DOCUMENTATION, SEGMENT, <https://segment.com/docs/engage/>.

<sup>24</sup> *Id.*

1 pages of the intake questionnaire and on all checkout screens.<sup>25</sup>

2 39. The Segment API captures patients' answers to the intake questionnaire on the  
3 Website, which includes information about patients' medical symptoms.

4 40. Twilio is able to identify each patient because the patient's name is disclosed by the  
5 Website during the checkout process.

6 41. The questionnaire is portrayed to Website visitors as an intake questionnaire used to  
7 obtain doctor-recommended, prescription hair loss products.<sup>26</sup>

8 42. Since at least May 2024, if not earlier, Keeps.com employed the Segment API on  
9 each page of the questionnaire and checkout process to track users' responses to the questions and  
10 send those responses to Defendant so Defendant can analyze the information and enable Keeps to  
11 target users with ads based on those answers.

12 43. By way of example, the images below show each page of the questionnaire. The  
13 Segment API is installed on each question.

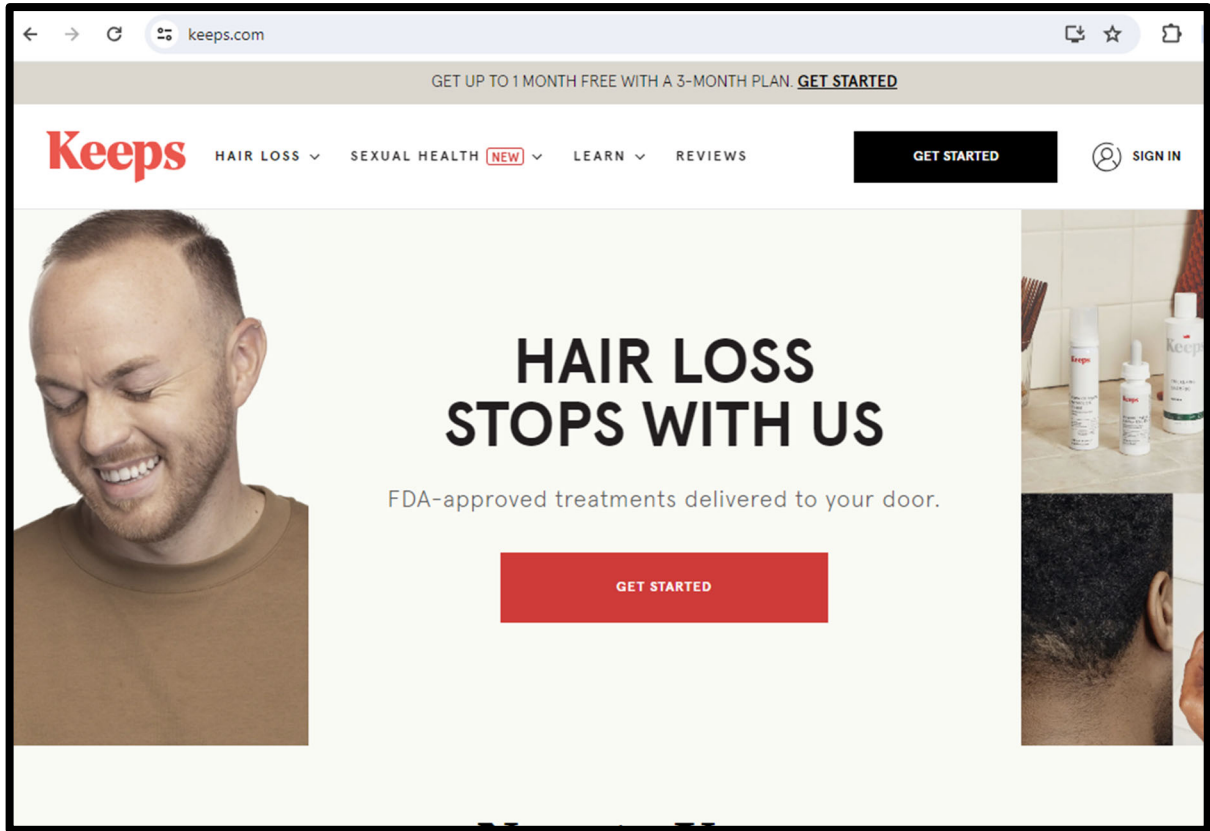
14 44. When visitors to the Website open the home page, they view a pop up with the title  
15 "HAIR LOSS STOPS WITH US" and the option to click a button to answer the questionnaire.  
16  
17  
18  
19  
20  
21  
22

---

23 <sup>25</sup> Keeps.com also offers sexual health medication. Website visitors purchasing sexual health  
24 medication enter information into the Website in a manner similar to the information entered to  
25 purchase hair loss medication. The Segment API is also installed on the pages related to the sexual  
26 health medication and collects visitors' communications in the manner described throughout this  
complaint. As such, all purchasers of sexual health medication on keeps.com are also Class  
Members.

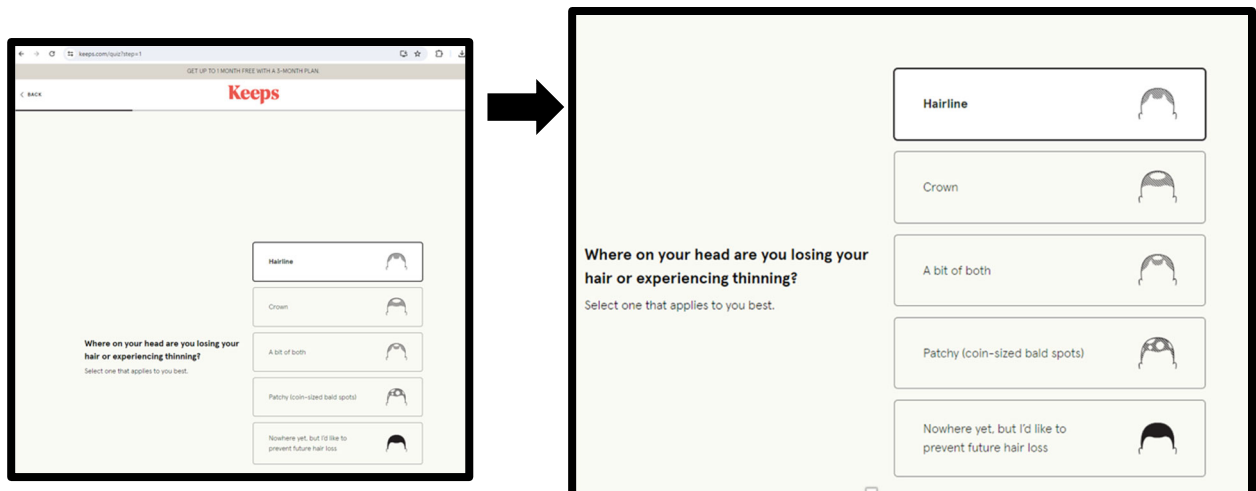
27 <sup>26</sup> Keeps.com also has a questionnaire for its erectile dysfunction products. The erectile  
28 dysfunction questionnaire functions the same as the hair loss questionnaire. Defendant's Segment  
API is also installed on each question of the questionnaire.

Figure 1



45. Clicking the “Get started” button directs users to the first question: “Where on your head are you losing your hair or experiencing thinning?” The Segment API is installed on this webpage and captures information about where the user is experiencing hair loss or thinning.

Figure 2



**Figure 3**

```


"path": "/quiz",
"referrer": "",
"referrer_url": "",
"segment_anonymous_id": "a13e6ff2-f00e-4deb-9481-8114465e98df",
"source": "keeps-next",
"windowSize": {
  "height": 902,
  "width": 1169
},
"action": "Mini Quiz Question Completed",
"category": "Mini Quiz",
"quizVersion": 2,
"recommendationVersion": "Mini Quiz LBS",
"label": "locationOfHairLossOnHead | Crown",
"nonInteraction": 1,
"quizQuestion": "locationOfHairLossOnHead",
"quizResponse": "Crown",
"utmCampaign": "google_search_branded_a1_exact_all-devices_fmf",

```

46. On the next page of the questionnaire, Keeps asks the visitor “Do you prefer taking pills or using topical treatments (foam /solutions/gels)?” The Segment API is installed on this webpage and captures information about where the user is experiencing hair loss or thinning.

**Figure 4**

**Do you prefer taking pills or using topical treatments (foams/solutions/gels)?**

 **WHY WE ASK THIS**

We offer treatments in several forms, and take your preferences into account. That said, we'll always recommend the most effective treatment for you, regardless of format.

Topicals (applied directly to head)

Pills (taken orally)

I'm not sure / I don't have a preference

**Figure 5**

```

"action": "Mini Quiz Question Completed",
"category": "Mini Quiz",
"quizVersion": 2,
"recommendationVersion": "Mini Quiz LBS",
"label": "treatmentType | Topicals (applied directly to head)",
"nonInteraction": 1,
"quizQuestion": "treatmentType",
"quizResponse": "Topicals (applied directly to head)",
"utmCampaign": "google search branded a1 exact all-devices fmf".

```

47. On the next page of the questionnaire, Keeps asks the visitor “Do you experience dandruff symptoms on your scalp? Flaking, itching, redness, or burning.” The Segment API is installed on this webpage and captures information about where the user is experiencing dandruff symptoms on their scalp.

**Figure 6**

Do you experience dandruff symptoms  
on your scalp? Flaking, itching, redness,  
or burning.

Yes

No



**Figure 7**

```
"action": "Mini Quiz Question Completed",  
"category": "Mini Quiz",  
"quizVersion": 2,  
"recommendationVersion": "Mini Quiz LBS",  
"label": "dandruffSymptoms | No",  
"nonInteraction": 1,  
"quizQuestion": "dandruffSymptoms",  
"quizResponse": "No",  
"utmCampaign": "google_search_branded_a1_exact_all-devices_fmf",
```

48. Through the Segment API, Defendant intercepts each of these communications in real time and sends the information to its own servers. Defendant then views each and every communication by Website visitors, stores the intercepted data on its servers in California, and processes the intercepted information for use in its advertised features as described above.

49. After completing the questionnaire, website visitors are recommended a treatment plan and are prompted to make an account. During the account creation process, Website visitors are prompted to enter their full name, email address, date of birth, and gender.

Figure 8

**Keeps**

YOUR PLAN ACCOUNT

### Personal Information

To ensure you're eligible for Keeps, we need a bit more information. This should only take a minute or two!

EMAIL\*  
Enter Your Email ⓘ  
Email is required.

PASSWORD\*  
Create Your Password ⓘ  
Minimum of 8 characters, including one special character.

SEX ASSIGNED AT BIRTH\* ⓘ STATE\*  
SELECT SEX ▼ SELECT STATE ▼

DATE OF BIRTH\*  
MM / DD / YYYY  
The date of birth provided must be the date of birth of the person signing up for treatment.

HOW DID YOU HEAR ABOUT US? (OPTIONAL)  
SELECT OPTION ▼

CONTINUE

### Your Treatment Plan Edit

**Topical Finasteride and Minoxidil Gel**  
3-month subscription  
~~\$180~~ **\$120**  
for your first order

**Ketoconazole Shampoo, 2%**  
3-month subscription  
~~\$33~~ **\$22**  
for your first order

50. These communications, which are related to Website visitors' treatment, are also intercepted in real time by Defendant via the Segment API.

Figure 9

```

},
"email": "thommy5432@yahoo.com",
"firstName": "Josiah",
"lastName": "Anderson",
"profileAttributes": {
  "dob": "07/19/1991",
  "gender": "male",
  "hearAboutUs": "Reddit"
}

```

1           51. By law, Plaintiff is entitled to privacy in his PHI and confidential communications.  
2 Defendant deprived Plaintiff of his privacy rights when it: (1) intercepted Plaintiff's and other  
3 online patients' confidential communications; and (2) undertook this pattern of conduct without  
4 notifying Plaintiff and without obtaining his express written consent. Plaintiff did not discover that  
5 Defendant intercepted his communications with keeps.com which contained PII and PHI to the  
6 Third Parties until May 2024.

7           **E. Twilio Wiretapped Plaintiff's Electronic Communications For Advertising,**  
8           **Marketing, And Analytics Purposes**

9           52. As described above, the Segment API collects information from visitors'  
10 interactions with keeps.com.

11           53. The purpose of this invasion of privacy is straightforward: Defendant collects  
12 information from keeps.com and sends back an analysis of that information, identifying website  
13 traffic and ad performance and targeting ads for specific individuals.

14           54. This is valuable to Defendants customers, like Keeps, because it improves the  
15 effectiveness of their advertisements, allows for the targeting of users, and provides performance  
16 information for ad campaigns.

17           55. In addition to helping companies like Keeps make better use of their own customer  
18 information, Defendant uses such information for its own purposes. Defendant's business model,  
19 based around the "Engage" profiles, requires that Defendant aggregate the information it intercepts  
20 from visitors of websites across the internet in order to create the hyper-specific consumer profiles  
21 described above. The creation of these aggregate profiles improves customer advertising  
22 campaigns on the "Engage Destinations" platforms and, thus, makes Defendant's services more  
23 valuable, enabling it to attract future customers. Thus, Defendant generates its own revenue by  
24 information mining internet activity and using that information for targeted advertising and  
25 building profiles of consumers to use in future advertising for new customers.

26           56. Thus, the agreement for Defendant to wiretap Plaintiff's and Class Members'  
27 communications on the Website is done for the purpose of improperly increasing the advertising  
28 efficacy and, by extension, profits of both parties.

**CLASS ALLEGATIONS**

57. Class Definition: Pursuant to Rule 23 of the Federal Rules of Civil Procedure, Plaintiff brings this action on behalf of himself and other similarly situated individuals defined as all persons in the United States who, during the class period, had their personally identifiable information or protected health information improperly disclosed to, and/or intercepted by, Defendant, as a result of using the Website (the “Class” or “Nationwide Class”).

58. Plaintiff also seeks to represent a subclass consisting of Class members who, during the class period, had their personally identifiable information or protected health information intercepted as a result of using the Website while located in California (the “California Subclass” or “Subclass”).

59. Plaintiff collectively refers to Class Members and Subclass Members as “Class Members,” unless it is necessary to distinguish between the two.

60. Plaintiff reserves the right to modify the class and subclass definitions or add additional subclasses as necessary prior to filing a motion for class certification.

61. The “Class Period” is the time period beginning on the date established by the Court’s determination of any applicable statute of limitations, after considering any tolling, concealment, and/or accrual issues, and ending on the date of entry of judgement.

62. Excluded from the Class and Subclass are Defendant; any affiliate, parent, or subsidiary of Defendant; any entity in which Defendant has a controlling interest; any officer director, or employee of Defendant; any successor or assign of Defendant; anyone employed by counsel in this action; any judge to whom this case is assigned, his or her spouse and immediate family members; and members of the judge’s staff.

63. Numerosity/Ascertainability. Members of the Class and Subclass are so numerous that joinder of all members would be unfeasible and not practicable. The exact number of Class and Subclass Members is unknown to Plaintiff at this time; however, it is estimated that there are thousands of individuals in the Class and Subclass. The identity of such membership is readily ascertainable from Defendant’s records and non-party records, such as those of keeps.com.

64. Typicality. Plaintiff's claims are typical of the claims of the Class and Subclass because Plaintiff used the Website and Defendant intercepted his PII without his express written authorization or knowledge. Plaintiff's claims are based on the same legal theories as the claims of other Class and Subclass Members.

65. Adequacy. Plaintiff is fully prepared to take all necessary steps to represent fairly and adequately the interests of the Class Members. Plaintiff's interests are coincident with, and not antagonistic to, those of the members of the Class and Subclass. Plaintiff is represented by attorneys with experience in the prosecution of class action litigation generally and in the emerging field of digital privacy litigation specifically. Plaintiff's attorneys are committed to vigorously prosecuting this action on behalf of the members of the Class and Subclass.

66. Common Questions of Law and Fact Predominate/Well Defined Community of Interest. Questions of law and fact common to the members of the Class and Subclass predominate over questions that may affect only individual members of the Class and Subclass because Defendant has acted on grounds generally applicable to the Class and Subclass. Such generally applicable conduct is inherent in Defendant's wrongful conduct. Questions of law and fact common to the Classes include:

- (a) Whether Defendant intentionally tapped the lines of internet communication between Plaintiff and the Website.
- (b) Whether Plaintiff's and Class Members' communications via the Website and the resultant interceptions thereof constitute an affirmative act of communication;
- (c) Whether Plaintiff and Class Members are entitled to damages under CIPA; and
- (d) Whether Defendant's actions violate Plaintiff's and Class Members' privacy rights as provided by the California Constitution.

67. Superiority. Class action treatment is a superior method for the fair and efficient adjudication of the controversy. Such treatment will permit a large number of similarly situated persons to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, or expense that numerous individual actions would engender. The benefits of proceeding through the class mechanism, including

1 providing injured persons or entities a method for obtaining redress on claims that could not  
 2 practicably be pursued individually, substantially outweighs potential difficulties in management of  
 3 this class action. Plaintiff knows of no special difficulty to be encountered in litigating this action  
 4 that would preclude its maintenance as a class action.

### 5 **COUNT I**

#### 6 **Violation of the California Invasion of Privacy Act** 7 **Cal. Penal Code § 631**

8 68. Plaintiff repeats the allegations contained in the paragraphs above as if fully set  
 9 forth herein and brings this count individually and on behalf of the members of the Class and  
 10 Subclass.

11 69. The CIPA is codified at Cal. Penal Code §§ 630 to 638. CIPA begins with its  
 12 statement of purpose – namely, that the purpose of CIPA is to “protect the right of privacy of the  
 13 people of [California]” from the threat posed by “advances in science and technology [that] have  
 14 led to the development of new devices and techniques for the purpose of eavesdropping upon  
 15 private communications . . . .” Cal. Penal Code § 630.

16 70. A person violates California Penal Code § 631(a), if:  
 17 by means of any machine, instrument, or contrivance, or in any other  
 18 manner, [s/he] intentionally taps, or makes any unauthorized connection,  
 19 whether physically, electrically, acoustically, inductively, or otherwise,  
 20 with any telegraph or telephone wire, line, cable, or instrument, including  
 21 the wire, line, cable, or instrument of any internal telephonic  
 22 communication system, or [s/he] willfully and without the consent of all  
 23 parties to the communication, or in any unauthorized manner, reads, or  
 24 attempts to read, or to learn the contents or meaning of any message,  
 25 report, or communication while the same is in transit or passing over any  
 26 wire, line, or cable, or is being sent from, or received at any place within  
 27 this state; or [s/he] uses, or attempts to use, in any manner, or for any  
 28 purpose, or to communicate in any way, any information so obtained . . . .

Cal. Penal Code § 631(a).

71. Further, a person violates § 631(a) if s/he “aids, agrees with, employs, or conspires  
 with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things  
 mentioned” in the preceding paragraph. *Id.*

72. To avoid liability under § 631(a), a defendant must show it had the consent of *all* parties to a communication.

73. At all relevant times, Defendant wiretapped Plaintiff's and Class Members' internet communications while accessing the Website. These communications were intercepted without the authorization and consent of Plaintiff and Class Members.

74. The following items constitute "machine[s], instrument[s], or contrivance[s]" under the CIPA, and even if they do not, the Segment API falls under the broad catch-all category of "any other manner":

- a. The computer codes and programs Twilio used to track Plaintiff's and Class Members' communications while they were filing out the questionnaire on the Website;
- b. Plaintiff's and Class Members' browsers;
- c. Plaintiff's and Class Members' computing and mobile devices;
- d. Twilio's web and ad servers;
- e. The web and ad servers from which Twilio tracked and intercepted Plaintiff's and Class Members' communications while they were filing out the questionnaire on the Website;
- f. The computer codes and programs used by Twilio to effectuate their tracking and interception of Plaintiff's and Class Members' communications while they were using a browser to visit the Website; and
- g. The plan Twilio carried out to effectuate their tracking and interception of Plaintiff's and Class Members' communications while they were using a web browser or mobile application to visit the Website.

75. The patient communication information that Defendant intercepted, respectively, such as information regarding Plaintiff's hair loss and hair regrowth expectations and prescription treatment for those conditions, constituted PHI.

76. As demonstrated hereinabove, Defendant violated CIPA by intercepting patients' online communications through the Website without their consent.

77. As a result of the above violations, Defendant is liable to Plaintiff and Class Members in the amount of the greater of \$5,000 dollars per violation or three times the amount of



1 actual damages. Additionally, Cal. Penal Code § 637.2 specifically states that “[it] is not a  
2 necessary prerequisite to an action pursuant to this section that the plaintiff has suffered, or be  
3 threatened with, actual damages.”

4 78. Under the statute, Defendant is also liable for reasonable attorney’s fees, and other  
5 litigation costs, injunctive and declaratory relief, and punitive damages in an amount to be  
6 determined by a jury, but sufficient to prevent the same or similar conduct by Defendant in the  
7 future.

8 **COUNT II**  
9 **Violation of the California Invasion of Privacy Act**  
10 **Cal. Penal Code § 632**

11 79. Plaintiffs incorporate the preceding paragraphs as if fully set forth herein.

12 80. Plaintiff Jonathon Perry-Hudson brings this claim against Defendant individually and  
13 on behalf of the Class.

14 81. CIPA § 632(a) prohibits an entity from:

15 intentionally and without the consent of all parties to a confidential  
16 communication, uses an electronic amplifying or recording device to  
17 eavesdrop upon or record the confidential communication, whether the  
18 communication is carried on among the parties in the presence of one  
19 another or by means of a telegraph, telephone, or other device, except a  
20 radio.

21 82. Twilio’s Segment API are “electronic amplifying or recording device[s].”

22 83. The following pieces of information provided by Plaintiff Perry-Hudson and  
23 California Class Members to the Website constitute “confidential communications”: Plaintiff’s  
24 symptoms and prescription medication to treat those symptoms. This information is, as described  
25 by the OCR in its bulletin, “highly sensitive.”

26 84. At all relevant times, Defendant intentionally used the Segment API to eavesdrop on  
27 the confidential communications of Plaintiff Perry-Hudson and Class Members.

28 85. When communicating with keeps.com, Plaintiff Perry-Hudson and Class Members  
had an objectively reasonable expectation of privacy. Plaintiff Perry-Hudson and Class Members  
did not reasonably expect that anyone other than keeps.com would be on the other end of the  
communication, and that other, third-party entities like Defendant would intentionally use an

1 electronic amplifying or recording device to eavesdrop upon and record the confidential  
 2 communications of Plaintiff and Class Members. Indeed, Plaintiff and Class Members each  
 3 communicated Personally Identifying Information (PII) and Protected Health Information (PHI) to  
 4 keeps.com as alleged above, which enhanced their reasonable expectation of privacy because such  
 5 secretive communications should not be disclosed to or intercepted by third parties like Defendant.

6 86. Plaintiff Perry-Hudson and Class Members did not consent to any of Defendants'  
 7 actions. Nor have Plaintiff or Class Members consented to Defendants' intentional use of an  
 8 electronic amplifying or recording device to eavesdrop upon and record the confidential  
 9 communications of Plaintiff and Class Members.

10 87. Pursuant to Cal. Penal Code § 637.2, Plaintiff Perry-Hudson and California Class  
 11 Members have been injured by Defendant's violations of CIPA § 632(a), and each seeks statutory  
 12 damages of \$5,000 for each of Defendant's violations of CIPA § 632(a).

### 13 **COUNT III**

#### 14 **Invasion of Privacy Under California's Constitution / Intrusion Upon Seclusion**

15 88. Plaintiff repeats the allegations contained in the foregoing paragraphs as if fully set  
 16 forth herein and brings this claim individually and on behalf of the members of the Class and  
 17 Subclass.

18 89. Plaintiff and Class Members have an interest in: (1) precluding the dissemination  
 19 and/or misuse of their sensitive, confidential communications and protected health information;  
 20 and (2) making personal decisions and/or conducting personal activities without observation,  
 21 intrusion or interference, including, but not limited to, the right to visit and interact with various  
 22 internet sites without being subjected to wiretaps without Plaintiff's and Class Members'  
 23 knowledge or consent.

24 90. At all relevant times, Defendant intentionally invaded Plaintiff's and Class  
 25 Members' privacy rights under the California Constitution, as well as intruded upon Plaintiff's and  
 26 Class Members' seclusion.

27 91. Plaintiff and Class Members had a reasonable expectation that their  
 28 communications, identities, health information, and other data would remain confidential, and that

1 Defendant would not wiretap the Website.

2 92. Plaintiff and Class Members did not authorize Defendant to intercept Plaintiff's and  
3 Class Members' private medical communications alongside their PHI and PII.

4 93. This invasion of privacy was serious in nature, scope, and impact because it related  
5 to patients' private medical communications. Moreover, it constituted an egregious breach of the  
6 societal norms underlying the privacy right.

7 94. Accordingly, Plaintiff and Class Members seek all relief available for invasion of  
8 privacy claims under California's Constitution and common law.

9 **PRAYER FOR RELIEF**

10 **WHEREFORE**, Plaintiff, on behalf of himself and Class Members, request judgment  
11 against Defendant and that the Court grant the following:

- 12 A. For an order certifying the Class and the Subclass under Rule 23 of the Federal Rules  
13 of Civil Procedure, naming Plaintiff as the representative of the Class and Subclass,  
14 and Plaintiff's attorneys as Class Counsel to represent the Class and Subclass  
15 members.
- 16 B. For equitable relief enjoining Defendant from engaging in the wrongful conduct  
17 alleged in this Complaint pertaining to the misuse and/or disclosure of the Private  
18 Information of Plaintiff and Class Members;
- 19 C. For an order finding in favor of Plaintiff, the Class, and the Subclass on all counts  
20 asserted herein;
- 21 D. For an award of damages, including, but not limited to, actual, consequential,  
22 statutory, punitive, and nominal damages, as allowed by law in an amount to be  
23 determined;
- 24 E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;
- 25 F. For prejudgment interest on all amounts awarded; and
- 26 G. Such other and further relief as this Court may deem just and proper.

27 **JURY TRIAL DEMANDED**

28 Plaintiff demands a trial by jury on all claims so triable.

1 Dated: June 21, 2024

**BURSOR & FISHER, P.A.**

2 By: /s/ Brittany S. Scott  
Brittany S. Scott

3  
4 Brittany S. Scott (State Bar No. 327132)  
Joshua R. Wilner (State Bar No. 353949)  
1990 North California Blvd., Suite 940  
5 Walnut Creek, CA 94596  
Telephone: (925) 300-4455  
6 Facsimile: (925) 407-2700  
E-mail: bscott@bursor.com  
7 jwilner@bursor.com

**BURSOR & FISHER, P.A.**

8 Philip L. Fraietta (State Bar No. 354768)  
9 1330 Avenue of the Americas, 32nd Floor  
New York, NY 10019  
10 Telephone: 646-837-7150  
Facsimile: (212) 989-9163  
11 E-Mail: pfraietta@bursor.com

**DRURY LEGAL, LLC**

12 Scott R. Drury (State Bar No. 355002)  
13 6 Carriage Lane  
Highwood, Illinois 60040  
14 Telephone: (312) 358-8225  
E-mail: scott@drurylegal.com

15  
16 *Attorneys for Plaintiff*  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28